의료기관 IT 보안 취약점 점검 및 대응방안

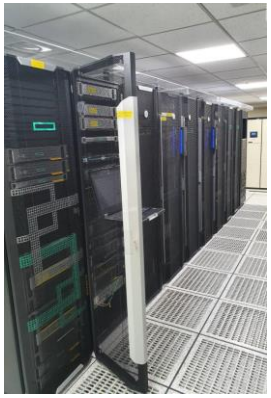
삼성서울병원
안 종 권

목차

병원 IT특징

IT 및 네트워크 **기술의 발달**로 다양한 의료서비스의 **정보화 환경으로 변경**되고 있어
IT 시스템 외 의료 장비 및 기기들이 신규 도입·운영 **시스템 관리가 어려운 환경으로 변화**

IT 시스템



홈페이지, 서버, DB, PC

다양한 의료 장비 및 기기

의료기기 600종

KIOSK, 약품조제 장비, 영상입력장비, 로봇

위협 및 사례

의료 기관 대상으로 해킹 공격 증가를 우려하며 매 년 해킹 사고가 증가 하는 추세
‘21년 미국 의료기관 대상으로 해킹 시도 확인 결과 사상 최고치 해킹 공격 시도가 확인

매년 해킹 공격 예상

코로나19 이후 의료시설 노린 사이버공격 45% 늘어

| 타 산업 대비 2배 증가…"분야 특성상 금전 지불 유인 높다고 판단"

컴퓨팅 | 입력 :2021/01/06 17:25 수정: 2021/01/06 17:27

일선 의료기관 원격접속 공격 768%급증...해킹 주의보

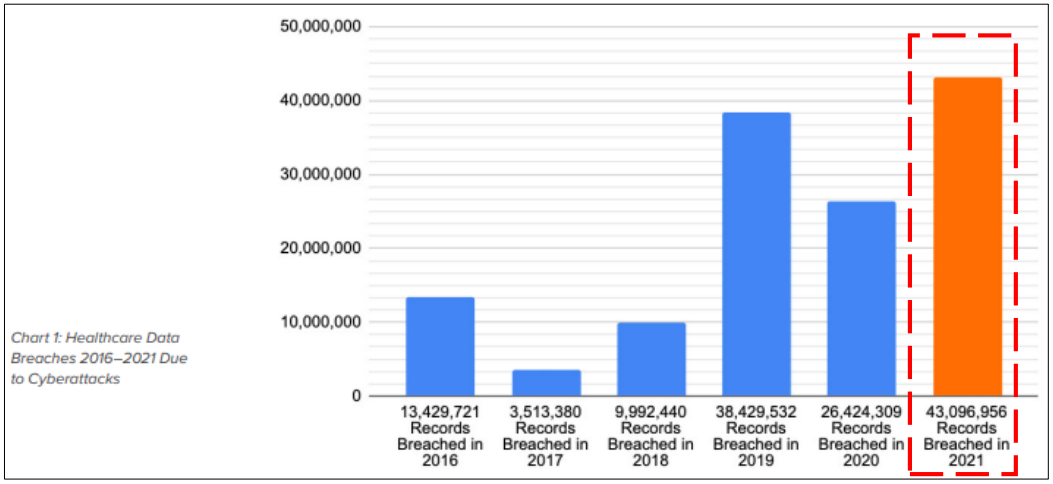


Chart 1: Healthcare Data Breaches 2016–2021 Due to Cyberattacks

위협 및 사례

의료기관 대상으로 해킹사고 발생되고 있으며 홈페이지, 의료기기, 스마트 기기, 클라우드 등 **다양한 의료 시스템에서 침해 및 감염 사례가 확인**되고 있음

해킹 사고 사례

PC부터 X-Ray까지...랜섬웨어 등 '병원 사이버 침해' 올해 11건

이승덕 기자 | 입력 2021.07.30 16:05 | 수정 2021.07.30 17:49 | 댓글 0

진료정보침해대응센터 의료기관 홈페이지 악성코드 확인 등 무상확인 가능

[의학신문·일간보사=이승덕 기자]의료기관에 연 10건이 넘는 '사이버 테러'가 발생하고 있어 주의가 당부된다.

30일 보건복지부 보침해대응센터(사고 신고·접수는 다.

지난해 총 13건(이 그 발생건수는

기관별로는 병원 서도 2건이 신고됐다. 이어 의원 2건, 종합병원 1건, 한방병원 1건

침해유형별로 보면 랜섬웨어가 9건으로 대부분이었는데(기타 2 DDoS 1건으로 랜섬웨어가 많았다.

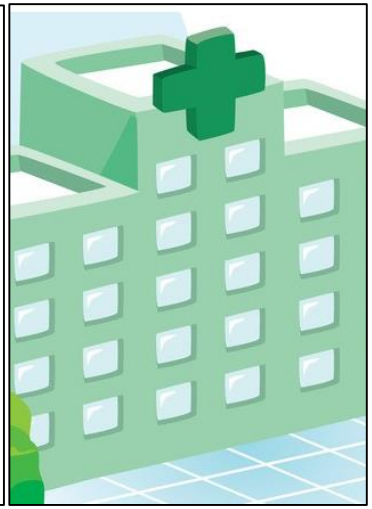
의료기관 해킹 사고 비상…의료기기 이어 '병원 자율로봇'도 노출

발행일 2022-04-16 10:00:02

'화이트 해커'인 버나비 잭은 2013년에 인슐린 펌프를 해킹하는 시연을 통해 당뇨 환자들의 혈당량을 치명적인 수준으로 끌어올리는 장면을 보여줬다. 이를 통해 의료 시스템이 해킹돼 당뇨뿐만 아니라 여러 질병을 앓는 환자들에게 치사량의 약을 투여하는 것이 얼마나 쉽게 일어날 수 있는 사고인지를 보여주고자 했다.

위협 및 사례

환자정보 보유 및 의료IT 기술력은 약하다는 인식으로 해커들 사이에서 좋은 공격 대상
의료기관 대상 해킹 공격이 증가하고 있어 해킹 사고 보안 대책 마련이 필요

환자정보 보유	개선 불가	의료기기 증가	피해 복구 절박
			

해킹 사고 보안 대책

- 침해사고 대응모의훈련을 통한 **보안 인식 제고**
- 보안 컴플라이언스 **준수 이상의 보안강화**
- 균형 있는 침해사고 **예방 및 대응 체계 마련**

IT 보안 점검

해킹사고 보안 대책에 따라 담당자를 선정하여 보안 점검을 실시, 도출된 취약점 개선
년 1회 이상 모의훈련, 모의해킹, 감염 사고 예방 활동 실시

[다양한 모의훈련]

❖ **악성 메일 모의 훈련**
- 의심 메일 신고 및 확인
- 모의 훈련 실시 및 교육

❖ **각종 침해사고 모의 훈련**
- 홈페이지 해킹사고 대응
- 개인정보 유출사고 대응

년 1회 이상 점검

[모의해킹 및 취약점 점검]

❖ **응용프로그램 보안 점검**
- 모의해킹
- 웹 취약점 자동 스캔
- 소스코드 진단

❖ **신규 오픈 시스템 보안 점검**
- 소스 변경 시스템 점검

❖ **테마 보안 점검**

년 1회 이상 점검

[해킹 및 감염 사고 예방]

❖ **백신 감염 분석**
- 악성코드 감염 분석 및 대응
- 불법 프로그램 사용 조사

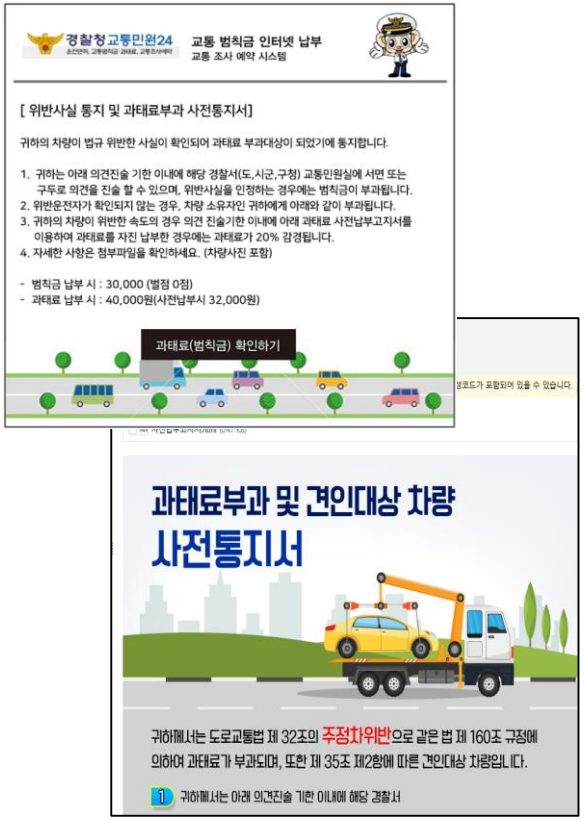
❖ **자체 보안관리**
- 해킹 IP 차단 및 공유
- 해킹 상세 분석 및 대응
- 각종 보안 패치 적용

상시 업무

IT 보안 점검_악성 메일 모의 훈련

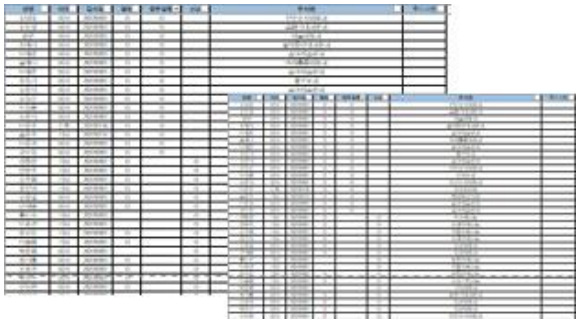
악성 이메일을 통한 랜섬웨어 및 악성코드 감염 사고가 지속적으로 증가
2015년부터 분기별로 임직원 보안 의식 제고를 위한 악성 이메일 모의 훈련을 실시

훈련용 샘플 메일 제작



첨부파일/링크 클릭 시 팝업 내용

훈련 결과 확인, 보안교육 실시



IT 보안 점검_악성 메일 모의 훈련

악성 이메일 모의훈련을 실시하고 결과를 분석하여 보안 교육이 필요한 인원 선정
첨부파일 클릭 및 메일 내 링크 클릭 대상자는 보안 교육을 통해 보안 의식 제고

모의훈련 결과

악성 메일 모의훈련
→ 첨부 실행률 감소
→ 의심 메일 신고 증가

신규 입사 기존 임직원 대비
첨부 실행률 높고, 신고 낮아

신규 입사자 집중 모의 훈련

보안 교육 실시

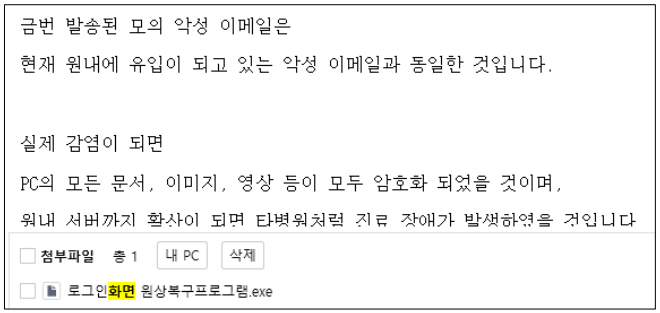
정교화된 악성 메일 유입 증가

보안팀 확인 요청 후 열람, 업무 외 메일 열람 금지

IT 보안 점검_악성 메일 모의 훈련

효과적인 악성 이메일 모의 훈련을 위해 악성 파일의 행위와 비슷한 첨부파일 제작
악성 메일 신고률 향상을 위해 모의 훈련 간 신고 임직원 포상, 보안 교육 실시

악성 메일 간접 체험(잠금화면 변경)



악성 메일 신고자 포상(커피 쿠폰)

첨부 실행률 감소 활동

- 첨부 실행 임직원 보안 교육 및 경고장 발부
- 첨부 실행률 높은 직종 대상 모의 훈련
- 효과적인 보안 교육을 위해 다양한 컨텐츠 계획

IT 보안 점검_악성 메일 신고 및 분석

의심 메일을 신고하면 보안 담당자는 해당 메일을 분석 후 신고자에게 안내 메일 발송
신고률 향상을 위해 월 1회 악성 메일 신고자 포상, 악성 메일 미 신고자 보안 교육 실시

원내 유입 악성 메일

Dear Supplier

I sent this ProForma Invoice earlier kindly check and inform me immediately before Payme

Please Find attachment on our company documentation business secured files link b

ProForma-Invoice.xlsx

Hi. I'm sorry I was away for the weekend.
It's ready.

Invoice Portal

Give me a call if you have any questions regarding the invoice.
Payment must be done in 48 hours.

Thank you!

Clifford Fettig

분석

차단

분석

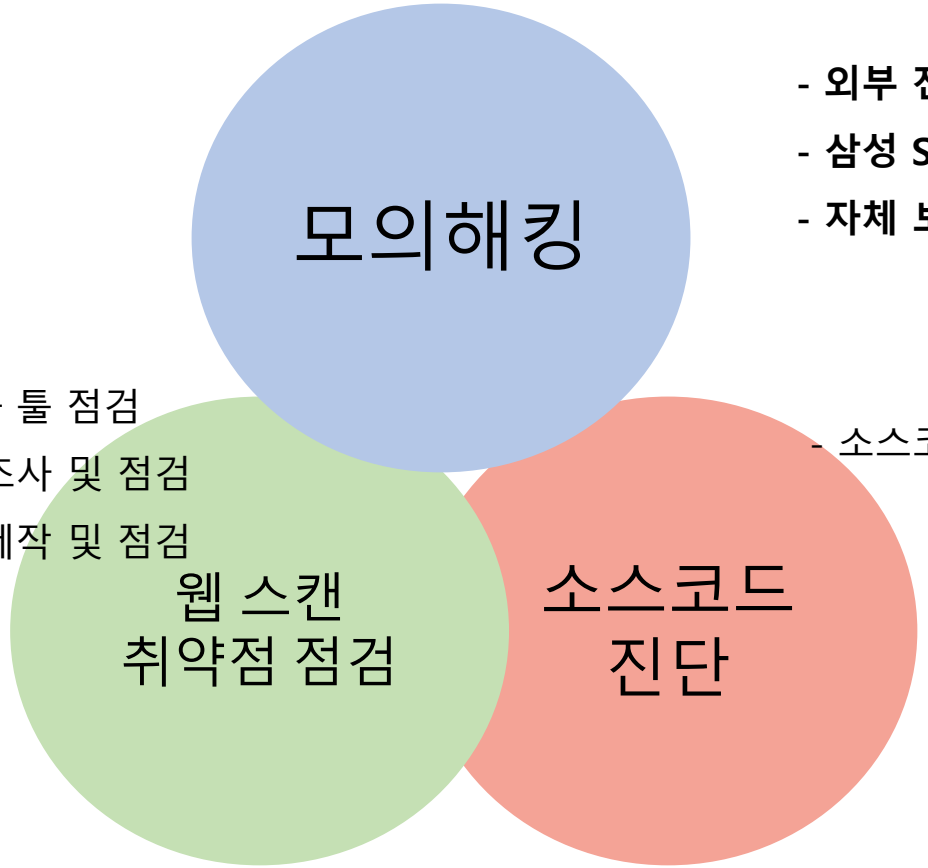
포상

악성 메일 신고 접수 후 진행사항

- 신고 메일 악성 여부 **분석 및 회신**
- 추가 유입 **차단** 및 전체 수신 메일 **삭제**
- 악성 메일 **원내 공지** 및 주의 요청
- 수신자 전체 확인 및 미신고 인원 **교육**

IT 보안 점검_응용프로그램 보안 점검

응용프로그램 보안 점검은 모의해킹, 웹 스캔 취약점 점검, 소스코드 진단으로 진행
년 2회 보안 점검을 진행하며 다양한 보안 점검 방식으로 취약점 도출하고 개선 노력



- **외부 전문 보안 업체 점검**
- **삼성 SDS 보안 점검**
- **자체 보안점검**

- 웹 스캔 자동화 툴 점검
- 신규 보안 툴 조사 및 점검
- 보안 점검 툴 제작 및 점검

- 소스코드 솔루션 점검

OWASP(open web application security project)점검 기준으로 보안점검을 실시

IT 보안 점검_응용프로그램 보안 점검

OWASP(Open Web Application Security Project)는 **오픈소스 웹 애플리케이션 보안 프로젝트**입니다.

OWASP처럼 애플리케이션 보안에만 전념하는 여러 커뮤니티 그룹의 조직이 상당히 커지고 있습니다. **OWASP는 가장 큰 오픈소스 웹 애플리케이션 보안 프로젝트로 주로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며, 10대 웹 애플리케이션의 취약점 (OWASP TOP 10)을 발표**합니다.

OWASP TOP 10은 웹 애플리케이션 취약점 중에서 빈도가 많이 발생하고, 보안상 영향을 크게 줄 수 있는 것들 10가지를 선정한 문서입니다.

OWASP Top 10 – 2013	OWASP Top 10 – 2017	OWASP Top 10 – 2021
A1 – Injection	A1 – Injection	A1 – Broken Access Control
A2 – Broken Authentication and Session Management	A2 – Broken Authentication	A2 – Cryptographic Failures
A3 – Cross-Site Scripting (XSS)	A3 – Sensitive Data Exposure	A3 – Injection
A4 – Insecure Direct Object References	A4 – XML External Entities (XXE)	A4 – Insecure Design
A5 – Security Misconfiguration	A5 – Broken Access Control	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Security Misconfiguration	A6 – Vulnerable and Outdated Components
A7 – Missing Function Level Access Control	A7 – Cross-Site Scripting (XSS)	A7 – Identification and Authentication Failures
A8 – Cross-Site Request Forgery (CSRF)	A8 – Insecure Deserialization	A8 – Software and Data Integrity Failures
A9 – Using Known Vulnerable Components	A9 – Using Components with Known Vulnerabilities	A9 – Security Logging and Monitoring Failures
A10 – Unvalidated Redirects and Forwards	A10 – Insufficient Logging & Monitoring	A10 – Server-Side Request Forgery

IT 보안 점검_응용프로그램 보안 점검

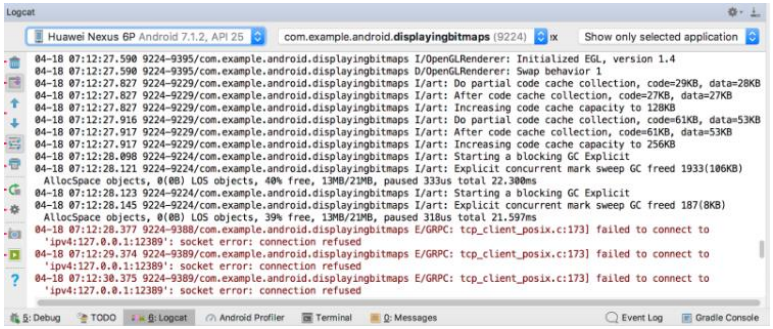
년 1회 이상 OWASP Mobile 기준으로 보안 취약점 점검을 실시, 사전에 보안 취약점을 확인하여 개선함으로써 보안 사고 방지

중요정보 유출

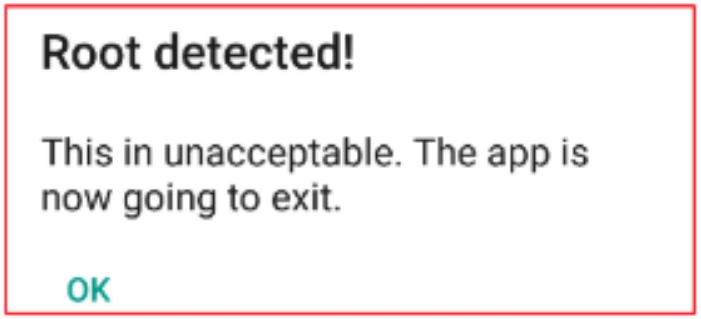
```
dream2qltechn:/mnt/sdcard # ls -al
total 76
drwxrwx--x 18 root sdcard_rw 4096 2022-01-11 22:24 .
drwx--x--x  4 root sdcard_rw 4096 2020-10-09 12:18 ..
drwxrwx--x  2 root sdcard_rw 4096 2020-11-19 01:31 .posteditor
-rw-rw----  1 root sdcard_rw   36 2020-11-16 15:39 .profig.os
drwxrwx--x  4 root sdcard_rw 4096 2020-12-02 16:35 .vkontakte
drwxrwx--x  2 root sdcard_rw 4096 2020-10-09 12:18 Alarms
drwxrwx--x  4 root sdcard_rw 4096 2020-10-09 17:51 Android
drwxr-xr-x  1 root sdcard_r    64 2020-10-09 12:18 BigNoxGameHD
drwxrwx--x  5 root sdcard_rw 4096 2020-11-16 15:44 DCIM
```

- /data/data 내 중요정보 저장
- sqlite DB 정보 노출
- 안드로이드 외부 저장소 관리 미흡

Log파일내 인증정보 평문저장(logcat 확인)



Rooting 체크 미흡 또는 부재



IT 보안 점검_신규 오픈 시스템 보안 점검

신규 오픈 시스템 점검 및 취약점 개선 후 오픈 가능, 다양한 스마트 및 의료기기 점검
기술이 발달함에 따라 다양한 스마트 기기가 오픈되고 있어 꾸준한 보안 역량 강화 필요

'15년 점검 대상

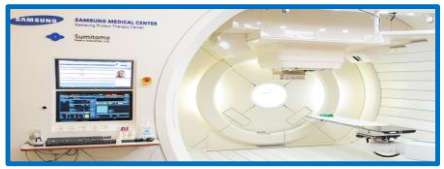
점검 대상

· 홈페이지/CS 프로그램

· 모바일 앱

'22년 신규 기술 접목 시스템 점검

✓ 다양한 병원 기반 운영 및 연계 시스템 보안 취약점 점검



✓ 의료 장비 IOT 취약점 점검

✓ 신규 스마트 기기 보안 취약점 점검

✓ **클라우드** 서비스 관리 점검 및 **운영 시스템** 정기적 점검

IT 보안 점검_취약점 개선 및 재발 방지

시스템 보안 점검을 도출된 보안 취약점 개선도 중요하지만 추 후에 동일한 취약점이 발생되지 않도록 전수검사 및 개발자 보안 교육을 통한 재발방지 또한 중요

소스 변경 시 보안성 검토

· 운영 시스템 소스 변경 보안 점검

· 신규 시스템 보안 점검

전체 메뉴 전수검사 지원

· 전체 점검 스크립트 제작 점검

· 자동 보안 시스템 점검

개발자 보안 교육

· **개발자 대상 보안 교육**

· **시스템 담당자 보안 교육**

→ 취약점 재발 방지

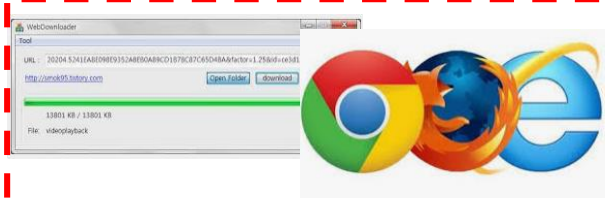
IT 보안 점검_백신 감염 분석

'21년 크게 증가한 제로데이 취약점 공격, 크랙 프로그램으로 위장하여 원내 유입한 악성코드 연이어 공개되는 오픈소스 보안 취약점에서 안전하게 지키기 위해 백신 감염 대응 활동 실시

백신 운영 관리

- 백신 설치률 관리
- 감염 USB 관리
- 크랙 프로그램 차단
- 중복 감염 임직원 관리

다운로드 파일 및 URL 분석



- 임직원 파일다운로드 분석
- 임직원 인터넷 접속 정보 분석

자체 분석(IDA, proceexp, wireshark)

- 악성파일 분석 및 패턴 업데이트

IT 보안 점검_자체 보안관리

공격자들의 수준이 크게 높아짐, 21년 제로데이 취약점을 이용한 공격이 크게 증가
각 기관에서 제공하는 해킹 공격 IP 및 자체 보안 솔루션 분석을 통해 확인된 IP 차단

해킹 IP 공유 제공

KISA
Korea Internet & Security Agency

의료기관공동보안관제센터
(의료ISAC)

C-TAS 정보공유시스템
Cyber Threat Analysis & Sharing system

해킹 및 악성 도메인, 오픈소스 취약점 공격
IP 수집 및 차단

자체 보안 솔루션 장비 운영

홈페이지 접근하는 의심 IP 선별/차단

IT 보안 점검_자체 보안관리

21년 제로데이 취약점을 이용한 공격이 폭발적으로 증가하고 있어 원내에서 사용중인 소프트웨어 패치 관리 및 PMS 관리되지 않는 프로그램에 대해서는 자체 관리 필요

패치 관리 중요성 증가

'21년 취약점 공개 SW

- 인터넷(IE), Adobe, Java, MS, 기타 순위로 CVE 취약점이 공개

· 정기 패치 적용 기간내 적용률 확인
· 정기적인 패치 관리 점검 실시
· 긴급 패치 적용 확인

신규 취약점 공개 모니터링

시스템으로 자동 패치 관리 불가

공개 취약점 모니터링 및 개선

IT 보안 점검_결론

의료기관 대상으로 해킹 및 악성코드 감염 공격이 증가, **현재 운영중인 보안 활동에서 부족한 부분이 없는지 확인 필요** 보안 담당자의 **사고 방지를 위한 관심과 노력**이 중요

[모의 훈련]	[모의해킹 및 취약점 점검]	[해킹 및 감염 사고 예방]
❖ 악성 메일 모의 훈련 ❖ 침해사고 모의 훈련	❖ 응용프로그램 보안 점검 ❖ 신규 오픈 시스템 보안 점검 ❖ 테마 보안 점검	❖ 백신 감염 분석 ❖ 자체 보안관리

개선, 취약점 확인 부족한 영역 보완

보안사고
해킹사고
악성코드감염
개인정보유출

예방활동 ✚

담당자
역량강화
사고방지
노력, 관심

Thank You